REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
12-01-2016	Final Report	1-Aug-2014 - 30-Apr-2015

4. TITLE AND SUBTITLE
Final Report: Formal Foundations for Wireless Network Agility

5a. CONTRACT NUMBER
W911NF-14-1-0389

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Ehab Al-Shaer

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of North Carolina - Charlotte
9201 University City Boulevard

Charlotte, NC 28223 -0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
64602-CS-II.2

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
Wireless is a key components in most today's network infrastructures. Yet, it is highly susceptible to networks attacks because wireless communication and infrastructure (such as Access point and clients) can be easily discovered and targeted. Particularly, the static nature of the wireless AP topology and its configuration offers a significant advantage to adversaries to identify network targets and plan devastating attacks such as denial of service or eavesdropping. This is critically important in hostile military environment in which soldiers depends on wireless infrastructure for communication and coordination More specifically, in the current structure of hotspot

15. SUBJECT TERMS
agility, wireless, MTD

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Ehab Al-Shaer
UU	UU	UU	UU		19b. TELEPHONE NUMBER 704-687-8663

Report Title

Final Report: Formal Foundations for Wireless Network Agility

ABSTRACT

Wireless is a key components in most today's network infrastructures. Yet, it is highly susceptible to networks attacks because wireless communication and infrastructure (such as Access point and clients) can be easily discovered and targeted. Particularly, the static nature of the wireless AP topology and its configuration offers a significant advantage to adversaries to identify network targets and plan devastating attacks such as denial of service or eavesdropping. This is critically important in hostile military environment in which soldiers depends on wireless infrastructure for communication and coordination.More specifically, in the current structure of hotspot wireless networks, the access point assignment as well as the traffic route between source and destination is fixed. This static AP association offers a significant advantage for adversaries to gather information and launch attacks such as eavesdrop or DoS attacks on certain network flows. There are a number of existing dynamic protocols in wireless networks such as randomized multi-path routing and node status scheduling.

The main objective of these protocols is to increase network resiliency in case of dynamic ad hoc network topology. However, in these protocols, the node status and route selection are predictable, which makes the network vulnerable to the adversary.This pro ject proposes a new layer of dynamicity using random AP mutation to increase the wireless agility and defense. The main objective of these techniques is to proactively mutate the wireless
network configuration and topology to deceive adversaries in their reconnaissance and intelligence gathering process and also to defend against link targeted attacks. The multipath algorithm can generate randomized multipath routes that are also highly dispersive and energy efficient in wireless sensor networks, but it only targets for single black hole attacks.

The goal of this project is to investigate formal foundations for two AP wireless agility techniques: (1) Random Range Mutation (RNM) that allows for periodic changes of AP coverage range randomly, and, (2) Random Topology Mutation (RTM) that allows for random motion and placement of APs in the wireless infrastructure. The goal of these techniques is to proactively defend against reconnaissance, and targeted attacks (e.g., DoS and eavesdropping attacks) by forcing the wireless clients to change their AP association and forwarding routes
randomly . One of the main challenges in this research is developing a formal framework that allows for optimize wireless agility while maintaining the end-to-end service requirements including reachability, security and QoS properties under incomplete information about the adversary strategies. The results of this research can be potentially extended to other wireless networks such as MANET and wireless SDN.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Access Point Mutation in Wireless Networks, Qi Duan, Linda Xie and Ehab Al-Shaer

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Fida Gilani	0.17	
Ghaith Husari	0.17	
FTE Equivalent:	**0.34**	
Total Number:	**2**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Qi Duna	0.33
FTE Equivalent:	**0.33**
Total Number:	**1**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Ehab Al-Shaer	0.08	
FTE Equivalent:	**0.08**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME
Total Number:

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Wireless communication and infrastructure, such as Access Point (AP) and clients, can be easily discovered and targeted. Particularly, the static nature of the wireless AP topology and its configuration offers a significant advantage to adversaries to identify network targets and plan devastating attacks such as denial of service or eavesdropping. This is critically important in hostile military environment in which soldiers depend on wireless infrastructure for communication and coordination.

In this project, we explored the formal foundation of novel wireless network mutation techniques that consider the adversary actions in order to maximize the benefit of network agility. Note that a complete random mutation could be too costly and even disruptive for network services. In addition, valid mutation is constrained by the availability of network resources such as signal power, number of APs, distribution of wireless clients, etc. Thus, one of the main challenges in this research is to develop a formal framework for effective wireless agility (e.g., low system and client overhead), while maintaining coverage, energy, and security (e.g., access control) constraints. We investigate formal foundations for two AP wireless agility techniques: (1) Random Range Mutation (RNM) that allows for periodic changes of AP coverage range randomly, and (2) Random Topology Mutations (RTM) that allows for random motion and placement of APs in the wireless infrastructure. The goal of these techniques is to proactively defend against reconnaissance and targeted attacks (e.g., DoS and eavesdropping attacks) by forcing the wireless clients to change their AP association and forwarding routes randomly . We show that we can use SMT to solve the wireless agility planning problems.

To the best of our knowledge, we are the first to propose AP mutation based wireless agility techniques. We believe that our work will enable the implementation of mutable wireless networks and motivate other kinds of moving target defense in wireless networks.

Our evaluation validates the feasibility, scalability, and effectiveness of the formal methods based technical approaches. We show that our SMT formalization can solve mutation scheduling in topologies as large as 2500 vertices, and the throughput reduction is less than 2%. Compared with the case of no mutation, the percentage of compromised flows can decrease by more than 90%.

Technology Transfer

Access Point Mutation in Wireless Networks

Qi Duan, Linda Xie and Ehab Al-Shaer
University of North Carolina at Charlotte
Charlotte, NC, USA

***Abstract*—Wireless is a key component in most of today's network infrastructures. Yet, it is highly susceptible to network attacks because wireless communication and infrastructure, such as Access Point (AP) and clients, can be easily discovered and targeted. Particularly, the static nature of the wireless AP topology and its configuration offers a significant advantage to adversaries to identify network targets and plan devastating attacks such as denial of service or eavesdropping. This is critically important in hostile military environment in which soldiers depend on wireless infrastructure for communication and coordination.**

In this paper, we present formal foundations for two wireless agility techniques: (1) Random Range Mutation (RNM) that allows for periodic changes of AP coverage range randomly, and (2) Random Topology Mutation (RTM) that allows for random motion and placement of APs in the wireless infrastructure. The goal of these techniques is to proactively defend against targeted attacks (e.g., DoS and eavesdropping) by forcing the wireless clients to change their AP association randomly. We develop a Satisfiability Modulo Theories (SMT) based formal framework that allows for optimizing wireless AP mutation while maintaining service requirements including coverage, security and energy properties under incomplete information about the adversary strategies. Our evaluation validates the feasibility, scalability, and effectiveness of the formal methods based technical approaches.

I. Introduction and Motivation

Wireless communications has become a key component in most of today's network infrastructures, both in military and commercial applications. Indeed, the surge in the demand for wireless communication has led to a major revolution in the wireless landscape. In the next few years, it is anticipated that a viral deployment of small-sized wireless base stations, known as *small cell base stations* (SBSs) will occur at a massive scale in order to lay the foundations of the next-generation 5G networks which can sustain the growth in the demand for the wireless capacity [6], [12], [20]. SBSs include a variety of access points (APs) such as picocells, femtocells, microcells, and macrocells, varying in coverage, capacity, and capabilities [6]. One of the key features of SBSs is their low-cost, low-coverage nature and their ability to be connected to any existing backhaul wired network such as DSL [20]. Such SBSs must co-exist with other wireless infrastructures such as WiFi APs, which are overlaid on top of this cellular architecture as shown in Fig. 1.

This massive network densification will lead to a major paradigm shift from current controlled, homogeneous wireless systems composed of sophisticated base stations or APs to decentralized, large-scale heterogeneous networks composed of cheap and small access points. A typical wireless network involves attaching several APs to a wired network and then providing wireless access to the LAN/WAN or another wireless

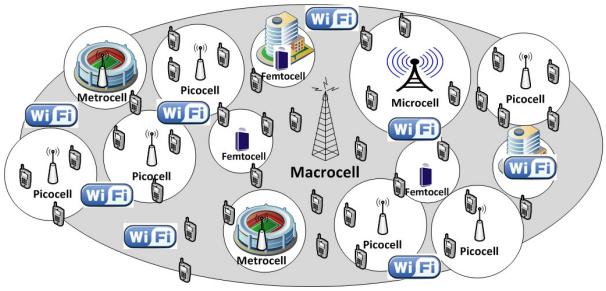

Fig. 1. An example of a large-scale, heterogeneous wireless network with various types of APs.

network. The wireless access points such as SBSs are managed by a controller that handles automatic adjustments to radio frequency power, channels, authentication, and security. The provision of security services in the wireless context faces a set of challenges that are specific to this new technology, which includes: a) small infrastructure nodes such as SBSs or small APs are more vulnerable to hacking than expensive and large base station towers, b) wireless communication and infrastructures (such as SBSs, WiFi access points, and even wireless clients) can be easily discovered and targeted, and c) SBSs and similar APs must connect to third party wired backhauls such as DSL, which can increase their vulnerability. More importantly, the static nature of the wireless AP topology in all existing infrastructure (cellular, unlicensed WiFi, or ad hoc) and its configuration offers a significant advantage to adversaries to identify network targets and plan devastating attacks such as denial of service or eavesdropping. This is critically important in hostile military environments in which soldiers depend on wireless infrastructure for communication and coordination. There are a number of existing dynamic protocols in wireless networks, such as randomized multi-path routing and wireless device status scheduling. The main objective of these protocols is to increase network resiliency in case of dynamic ad hoc network topology [16], [22]. However, in these protocols, the wireless device status and route selection are predictable, which makes the network vulnerable to the adversary.

In this paper, we explore wireless network mutation techniques that consider the adversary actions in order to maximize the benefit of network agility. Note that a complete random mutation could be too costly and even disruptive for network services. In addition, valid mutation is constrained by the availability of network resources such as signal power, number of APs, distribution of wireless clients, etc. Thus, one of the main challenges in this research is to develop a formal framework for effective wireless agility (e.g., low system and client over-

head), while maintaining coverage, energy, and security (e.g., access control) constraints. We investigate formal foundations for two AP wireless agility techniques: (1) Random Range Mutation (RNM) that allows for periodic changes of AP coverage range randomly, and (2) Random Topology Mutations (RTM) that allows for random motion and placement of APs in the wireless infrastructure. The goal of these techniques is to proactively defend against reconnaissance and targeted attacks (e.g., DoS and eavesdropping attacks) by forcing the wireless clients to change their AP association and forwarding routes randomly . We apply an SMT based approach to solve the wireless agility planning problems. SMT is a powerful tool to solve constraint satisfaction problems arise in many diverse areas, including software and hardware verification, type inference, extended static checking, test-case generation, scheduling, planning, graph problems, etc. [8].

To the best of our knowledge, we are the first to propose AP mutation based wireless agility techniques. We believe that our work will enable the implementation of mutable wireless networks and motivate other kinds of moving target defense in wireless networks.

The rest of the paper is organized as follows. Section II discusses the network and threat model used in the paper. Section III and IV present the problem definitions and technical approaches respectively. Implementation details are discussed in Section V. Evaluation results are presented in Section VI. Section VII presents related works and Section VIII concludes the paper.

II. System and Adversary Model

A. System Model

The network model in this paper conform with the following conditions:

(1) The wireless network has a number of APs, which may have dynamic configurations. An individual AP can provide connection to devices in its wireless radio range and is connected to one or more gateways or other APs (interconnected APs are similar as wireless ad hoc networks). A wireless device may be inside the range of multiple APs. The AP mutation (through configuration change) is controlled and regulated by a central controller.

2) Every AP can obtain its location in movement through GPS, which is the common situation for military wireless networks.

(3) We consider managed wireless networks where every AP has a unique identity. In other words, the mapping between AP nodes and their identities remains one-to-one, a property that can be verified in any managed network. This will preclude AP replication or spoofing attacks.

B. Threat Model

The following are the main assumptions when we consider the adversary:

(1) An adversary has limited amount of resources that are deployed in the network. We consider two capabilities for the adversary: eavesdropping and jamming. An adversary can deploy a number of attacking nodes in the network. Since APs in overlapped ranges will use different radio frequencies, we assume that every attacking node has the ability to eavesdrop or block (through jamming) only one AP in its range in a given time interval.

(2) An adversary may compromise a number of APs. However, she does not control certain elements such as mobility of the APs or modification/addition of the hardware of the captured APs. This assumption is perfectly legitimate since our model considers that the adversary does not know all the details of the network and it will exponentially increase the cost of gathering these details.

III. Problem Definition

Random Range Mutation (RNM). Randomly changing AP range forces wireless clients to switch their associated APs and routes. Thus, eavesdropping or DoS attackers who are targeting specific APs or clients will be confused since APs (as well as client associations) appear and disappear randomly and frequently. Also adversaries can not make any assumption about the client association with APs based on physical location. For instance, a client could be associated to an AP that is further than another AP based on the assigned range, which also dynamically changes. We assume that there is enough APs that can collaboratively cover the target area but in different ways. Note that one special case of AP range mutation is that multiple APs that are in close physical locations turn on/off alternately. Turning an AP off is equivalent to reducing its range to 0.

The RNM problem can be formally defined as follows. Suppose that the set of users in the wireless network is denoted as $\mathcal{P} = \{p_1, \ldots, p_z\}$. In this network, a set $\mathcal{N}$ of N range adjustable APs $\{s_1, s_2, \ldots, s_N\}$ is present. Every AP s_i has g_i possible ranges, denoted by the set

$$\mathcal{S}_i = \{\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ig_i}\}.$$

When s_i is set to be in range α_{ij} $(1 \leq j \leq g_i)$, it covers a subset $\mathcal{Y}_{ij}$ of users within the set $\mathcal{P}$, and the energy consumption rate is given by a function $f_i(\alpha_{ij})$. For an effective RNM, our goal is to find a range mutation schedule (range value, starting and ending time) for each AP that satisfies the following constraints:

- *Coverage constraint:* coverage of wireless users must be maintained.
- *Unpredictability constraint:* increasing unpredictability by minimizing the similarity between new and old mutation.
- *Capacity constraint:* the number of users that handled by every AP should not exceed the AP's capacity.
- *Energy constraint:* optimize energy consumption, because different range for the wireless APs will lead to different energy consumption rate.

Random Topology Mutation (RTM). The topology mutation is based on mobile APs that change their positions in random manner but with constraints. When a wireless AP changes its position, some wireless users may need to change its associated AP, and change forwarding routes accordingly. By moving the positions of the APs, we can achieve better security with limited number of APs. The objectives of random topology mutation are (1) to make wireless infrastructure resilient against infrastructure reconnaissance attacks, (2) to defend against physical attacks and increase the resilience to wireless device failures, which is particularly important for military applications, (3) to make eavesdropping attacks that are targeting specific clients extremely difficult as the attacker has to chase not only the mobility of client but also the mobility of the AP, and (4) to make wireless resilient against internal attacks in case some APs are compromised, because (a) one AP alone cannot focus on tracking or attacking (e.g., eavesdropping) a specific client as each AP will be constantly moving and the harm will be naturally distributed, and (b) the agile AP enables clients to compare the performance across various APs and potential detect malicious APs (e.g., one AP drops packets maliciously).

The topology mutation can be done in two scheduling phases. The first phase is to determine the satisfiable deployment of the APs for the next interval, and the second phase is to determine the detailed moving steps to move the APs from the current deployment to the new deployment. For the first phase, the following constraints should be satisfied for random AP deployment:

- *Coverage constraint:* coverage of wireless users must be maintained.
- *Unpredictability constraint:* increasing unpredictability by minimizing the topology similarity between new and old topology.
- *Capacity constraint:* the number of users that handled by every AP should not exceed the AP's capacity.

For the second phase, the major constraints are

- *Step constraint:* the total number of moving steps needed for the transition should be no more than some threshold value.
- *Energy constraint:* the total energy cost for moving from the old deployment to the new deployment should be less than some threshold.

IV. Technical Approaches

A. Preliminary Formalization and Constraints

1) Random Range Mutation: Random range mutation can be pre-calculated and staged in wireless APs in advance and activated based on moving target requirements. Intuitively, it is an optimization problem that can be solved using SMT solvers.

The following equation specifies the energy consumption upper bound (E_i) for every AP s_i (*energy constraint*):

$$\sum_{1\leq j\leq T} \omega_{ij} f_i(\omega_{ij}) \leq E_i,\ \forall i \in [1..N] \tag{1}$$

Here the variable ω_{ij} denotes the range of AP s_i at time interval j. The range can be one of $\alpha_{i1}, \ldots, \alpha_{ig_i}$, which can be represented by natural numbers. For example, we can use numbers $1, 2, \ldots, g_i$ to represent $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ig_i}$, respectively.

To set the choice of values of variable ω_{ij}, we need the following equation.

$$\omega_{ij} \in \{\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ig_i}\},\ \forall i \in [1..N], \forall j \in [1..T] \tag{2}$$

The following equation guarantees that every user should be covered by at least one AP in any time interval (*coverage constraint*).

$$\Big(\bigvee_{(i,u)\in\{(i,u)|p_k\in\mathcal{Y}_{iu}\}} \omega_{ij} = \alpha_{iu}\Big),\ \forall k \in [1..z], \forall j \in [1..T] \tag{3}$$

The next equation guarantees that the range of every AP in any time interval will be different from the previous time interval (*unpredictability constraint*).

$$\omega_{ij} \neq \omega_{i(j+1)},\ \forall i \in [1..N], \forall j \in [1..T-1] \tag{4}$$

Note that the unpredictability constraint can be flexible. One can require that the range of an AP must change over a number of time intervals (not necessarily two consecutive intervals).

Suppose the capacity of AP s_i (the maximum number of wireless users that can connect to it) is Q_i. Then the *capacity constraint* can be formalized as follows

$$\sum_{1\leq i\leq N} v_{ijk} = 1,\ \forall j \in [1..T], \forall k \in [1..z] \tag{5}$$

$$(v_{ijk} = 1) \Rightarrow \exists u((p_k \in \mathcal{Y}_{iu}) \wedge (\omega_{ij} = \alpha_{iu})),\ \forall i \in [1..N], \forall j \in [1..T], \forall k \in [1..z] \tag{6}$$

$$\sum_{1\leq k\leq z} v_{ijk} \leq Q_i,\ \forall i \in [1..N], \forall j \in [1..T] \tag{7}$$

In the above equation, $v_{ijk} = 1$ means that user p_k is assigned to AP s_i in interval j. Equation 5 guarantees that every user will be assigned with one AP. Equation 6 guarantees that when a user node is assigned by an AP, it should be inside the active range of the AP in the current interval. Equation 7 guarantees that every AP will not exceed its capacity.

2) Random Topology Mutation: In random topology mutation, the following formalization guarantees that every user should be covered by at least one AP for the deployment in the next interval (*coverage constraint*).

$$\Big(\bigvee_{(i,j)\in\{(i,j)|p_k\in\mathcal{Y}_{ij}\}} \omega_i = \alpha_{ij}\Big),\ \forall k \in [1..z] \tag{8}$$

In the above equation, the variable ω_i denotes the position of AP s_i in the next deployment. The choice of values of variable ω_i is defined by

$$\omega_i \in \{\alpha_{i1}, \ldots, \alpha_{im}\},\ \forall i \in [1..N] \tag{9}$$

In the above equation, $\{\alpha_{i1}, \ldots, \alpha_{im}\}$ are the possible locations that AP s_i can move to.

The *unpredictability constraint* can be formalized as follows:

$$\sum_{1 \le i \le n} \Delta_i \ge \delta \tag{10}$$

$$(\Delta_i = 1) \Leftrightarrow (\omega_i = \eta_i),\ \forall i \in [1..N] \tag{11}$$

$$\Delta_i \in \{0, 1\},\ \forall i \in [1..N] \tag{12}$$

In the above equations, δ is the overlap threshold (the minimum number of APs that should change location), and η_i is the old position of AP s_i. The unpredictability constraint guarantees that the number of moved APs in consecutive intervals should exceed a certain threshold.

The capacity constraint can be defined similarly as that in random range mutation.

In the second phase of topology mutation scheduling, suppose the maximum number of steps (one step means moving from a location to an adjacent location) required for the transition is b, we can formalize the *step constraint* as follows:

$$(\omega_{i1} = \eta_i) \wedge (\omega_{ib} = \overline{\eta_i}), \forall i \in [1..N] \tag{13}$$

$$(\omega_{i(j+1)} = \omega_{ij}) \vee (\omega_{i(j+1)} \text{ neighbor to } \omega_{ij}),$$
$$\forall i \in [1..N], \forall j \in [1..b-1] \tag{14}$$

In the above equations, η_i is the position of s_i in the original deployment, and $\overline{\eta_i}$ is the position of s_i in the new deployment. ω_{ij} denotes the position of s_i in step j. From step 1 to step $b-1$, we require that every movable AP should either remain in the previous position or move to a neighboring position.

Assume that every move in one step consumes one unit energy, we can formalize the *energy constraint* as follows:

$$\sum_{1 \le j \le b-1} \zeta_{ij} \le E_i, \forall i \in [1..N] \tag{15}$$

$$(\omega_{i(j+1)} \ne \omega_{ij}) \Leftrightarrow (\zeta_{ij} = 1),\ \forall i \in [1..N], \forall j \in [1..b-1] \tag{16}$$

$$\zeta_{ij} \in \{0, 1\},\ \forall i \in [1..N], \forall j \in [1..b-1] \tag{17}$$

In the above equations, E_i is the threshold for energy consumption for AP s_i and ζ_{ij} denotes whether AP s_i moves in step j or not.

V. Implementation

A. Protocol Overview

We propose a protocol to implement the proposed AP mutation schemes. In our proposed network architecture, a centralized controller is connected to all the APs in the network. This centralized controller acts as a radio resource coordinator across the network and takes care of issues related to AP coverage range mutation and random movement and placement. Note that the centralized controller is not necessarily an additional separate device. Instead, the functions of the controller can be implemented in an existing AP, and this AP becomes the controller of all APs.

The centralized controller gathers the measured signal and resource utilization statistics from all the APs via the backbone network connecting all the APs using Simple Network Management Protocol (SNMP) [14]. SNMP also provides security related functions such as user authentication and message encryption [9]. Most enterprise-class APs can support SNMP [17]. APs collect signal characteristics from wireless users. Based on IEEE 802.11k [4] radio resource measurement, signal characteristics can be obtained directly from the wireless network.

The controller and APs periodically collect the required information for AP mutation. The controller calculates the optimal range mutation schedule or the optimal AP deployment and movement schedule and sends decisions to APs. Due to the dynamics in the RF environment, signal characteristics, traffic load, and interference intensity are time-variant. As a result, the decision-making is updated periodically in order to reflect the influences of the time-varying environment. The signaling overhead caused by the proposed AP mutation schemes comes from the periodic measurement collection of the AP load and signal statistics from all APs to the controller. However, the traffic load at APs does not vary frequently, if users are not highly mobile. In addition, it is important to remark that the periodic data-collection does not imply measuring instantaneous small-scale multipath signal characteristics which are very time-sensitive. Instead, measurements should be targeted at capturing large-scale changes in signal characteristics due to variations in traffic pattern, user mobility, interference sources, and interference mobility. Thus, the signaling overhead that results from the periodic updating can be kept at a reasonable level. Generally speaking, the shorter the measurement interval, the more often the optimization decision is updated, the better performance the system can achieve in terms of wireless agility and load balancing based on the most recent traffic load and interference information, but the higher the signaling overhead.

The proposed protocol includes three steps. First, the controller collects the AP coverage information as well as the overall traffic load distribution and user distribution at all APs. Second, the controller finds the optimal mutation schedule (either range mutation or topology mutation) for each AP. In other words, the controller decides which AP should use which transmission power level to cover which range or which AP should move to which location. This optimal mutation schedule satisfies all the constraints. Finally, the controller sends control decisions to APs to instruct them on how to update their coverage ranges or locations. Therefore, by the control of the centralized controller on restricting the range or topology of APs, the network agility can be maximized, while user coverage, network capacity, and energy consumption constraints are not compromised.

B. Handoff in AP Mutation

One of the major challenges in this work is to maintain existing connections during the mutation. To achieve this, we must switch the association of the wireless node from one AP

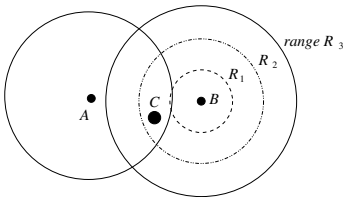

Fig. 2. An example of handoff

to another AP. To achieve a smooth switch, one can use soft handoff. Note that the soft handoff we apply here is a kind of proactive handoff caused by mutation. In the traditional cellular network, handoff is caused by the movement of the phone users, or when the capacity for connecting new calls of a given cell is used up, or user behavior changes. For example, when a fast-traveling user connected to a large umbrella-type of cell stops, the call may be transferred to a smaller cell in order to free capacity on the umbrella cell for other fast-traveling users and to reduce the potential interference. For the proactive handoff caused by range mutation, the handoff happens even when the wireless user is not moving.

As an example, in Fig 2, wireless node C is in the maximum range of wireless AP A and B. In interval T_1, B has range R_3 and C is associated with B. When AP B shrinks range from R_3 to R_2 in the next interval T_2, C finishes the handoff procedure to switch to AP A. In time interval T_3, B shrinks range to R_1 and C is now associated with A. Note that the handoff needs the cooperation of both APs. When there is no malicious activity, the handoff can happen smoothly without interrupting any existing connections. In the scenario when some APs are under DoS attack (such as jamming), the wireless node may directly switch to a new AP that is not under attack and old connections may be interrupted.

We can use the IAPP (Inter-Access Point Protocol) [1] for soft handoff. IAPP (standardized in IEEE Std 802.11f) is the IEEE standard for inter-access point communication. IAPP enables (fast) link layer re-association at a new access point in the same hotspot.

VI. Evaluation

A. Evaluation Metrics

For the benefit of AP mutation, we use the metric **Mutation Protection Effectiveness** (MPE) similarly as that used in [10] to evaluate the effectiveness of AP mutation against eavesdropping and DoS attacks. MPE is defined to be the percentage of packets in a flow that are eavesdropped or blocked by attackers. Obviously the requirement for minimum MPE is application dependent. For the cost of mutation, we measure (1) the time of the SMT solver to solve the formalizations and (2) the delay and throughput degradation caused by the mutation.

B. Evaluation Methodology

We use Yices [3] to solve the SMT formalizations. Yices is an SMT solver which can be used to solve constraint satisfaction problems in many diverse areas. For AP range mutation, we consider an area of 1000 by 1000 meters. APs

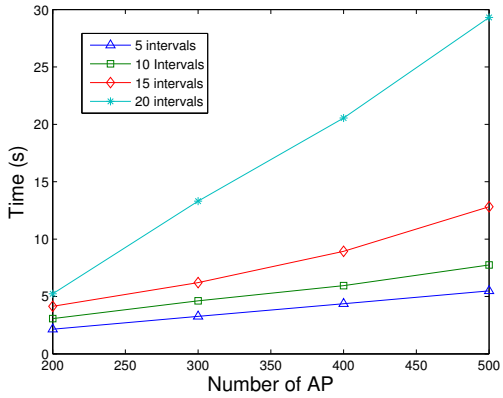

Fig. 3. Time to schedule multiple intervals

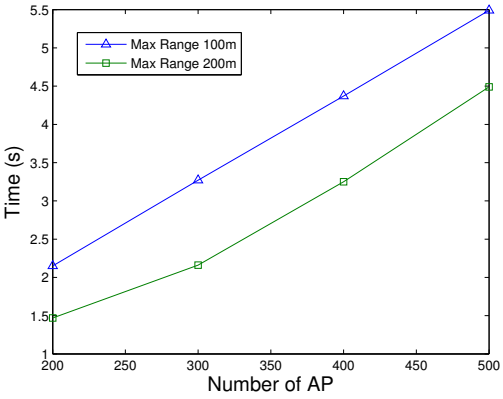

Fig. 4. Time to schedule APs with different ranges

are evenly distributed in the area. For an AP with maximum range R, it can adjust the range to be three levels, R, $R/2$ and 0. Range 0 means it is asleep. We also consider the wireless coverage for the grid points by dividing area into 100 cells where every cell has size 100m by 100m. In total there are $11 \times 11 = 121$ grid points.

SMT Solving Time of Range Mutation with Different Number of AP and Intervals: Fig 3 shows the time for the SMT solver to find the satisfying AP scheduling with different number of APs and intervals. In this figure and Fig 4, we consider the coverage of grid points. We can see that the time is increasing almost linearly with the increasing of APs.

SMT Solving Time of Range Mutation with Different Max Ranges: Fig 4 shows the time for the SMT solver to find the satisfying AP scheduling with different number of APs and maximum AP ranges. We can see that the time decreases with the increase of maximum AP ranges. This is because larger AP range makes it easier to satisfy the coverage requirements.

Average Number of Handoffs in AP Range Mutation: Fig 5 shows the average and standard deviation of the number of user handoffs during 30 intervals. There are 200 APs randomly deployed in the 1000 by 1000 meter region, and the max AP range is 150m. There are 1000 user nodes that

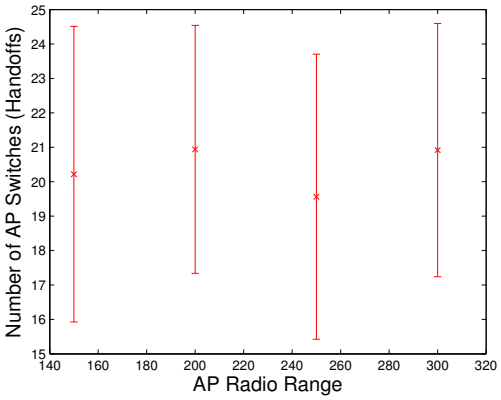

Fig. 5. Average number of handoffs

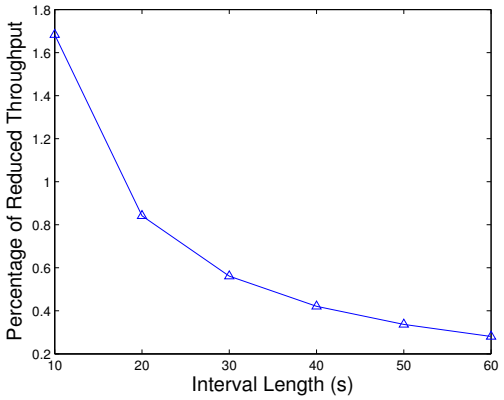

Fig. 7. Delays caused by handoffs

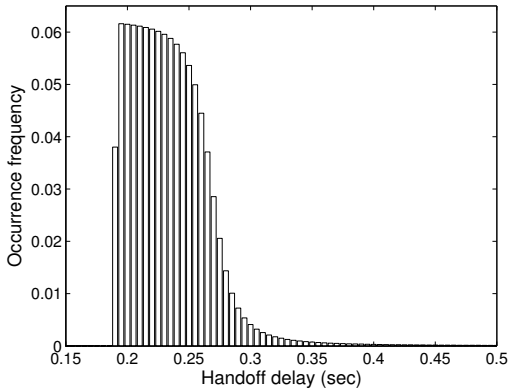

Fig. 6. Handoff delay distribution

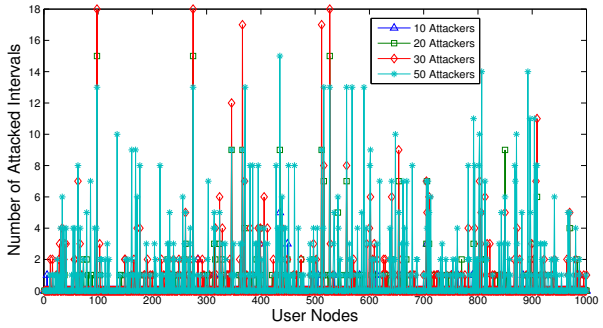

Fig. 8. Number of attacked intervals for every user

are randomly distributed in the region and all of them need to be covered by at least one active AP in any interval. We can see that in average there are about 20 handoffs for every user during the 30 intervals.

Average Throughput Reduction Caused by Handoffs: We use the analysis method proposed in [21] to generate each handoff delay. The total handoff delay includes the link-layer handoff delay and the network-layer handoff delay if the two APs are involved in a handoff. The link-layer handoff delay includes the channel scanning delay, authentication delay, and re-association delay [19]. The network-layer handoff delay includes the network-layer signaling message processing and transmission delay, the wireless access delay of the signaling messages, and the propagation delay. Based on the analysis in [21], the values of each handoff delay are random. As shown in Fig 6, under 99.3% of the cases, the handoff delay varies in the range between 0.18 and 0.4 seconds and the average is about 0.25 seconds. So we choose 0.25 second as the average handoff delay in the analysis for AP mutation. Fig 7 shows the average throughput reduction caused by handoffs during 30 intervals. We can see that the throughput reduction is small (less than 2 percent) for mutation interval length of 10 seconds. Clearly this is an acceptable cost for the mutation.

Number of Attacked Intervals: Fig 8 shows the number of attacked intervals for different number of attacking nodes. Here we also assume the attacking nodes are randomly distributed in the region. When an AP is within the range of any attacker node's radio range (also set to be 150m, same as the AP range), then we consider any user node that is associated with the AP is under attack. We can see that for most users the number of attacked intervals is less than 10 during the 30 intervals. Note that a similar analysis can be done for compromised APs. If an AP is compromised, any user session that is associated with it will be considered compromised.

Number of Impacted User Flows: Here we assume that every user has a session flow that lasts for 30 intervals and if the number attacked intervals is more than 10, we consider the flow is impacted or compromised. Fig 9 shows the number of compromised flows in two cases, with and without AP range mutation. For the case without AP mutation, any user node is randomly assigned to an available AP and the association is fixed during the whole 30 intervals. We can see that the difference between the two cases is significant.

For AP topology mutation, we use random planar topology generated by triangular graphs. Fig 10 shows the full triangular graph of 25 vertices, while Fig 11 and Fig 12 show the triangular graph with 10% and 25% of the edges randomly removed. Here we only choose the random graphs that are connected and all vertices have degree more than 1. The APs are randomly distributed in the vertices of the graph. Every

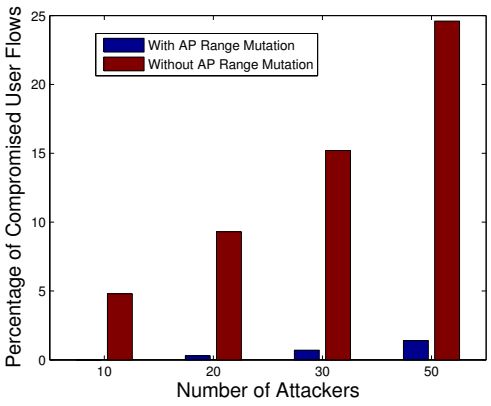

Fig. 9. Impacted User Flows

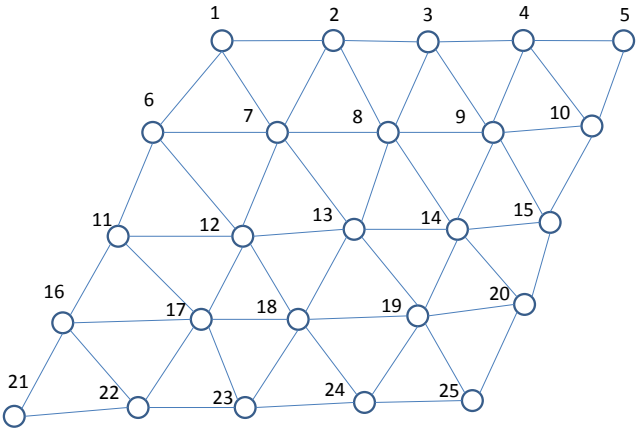

Fig. 10. Triangular Topology

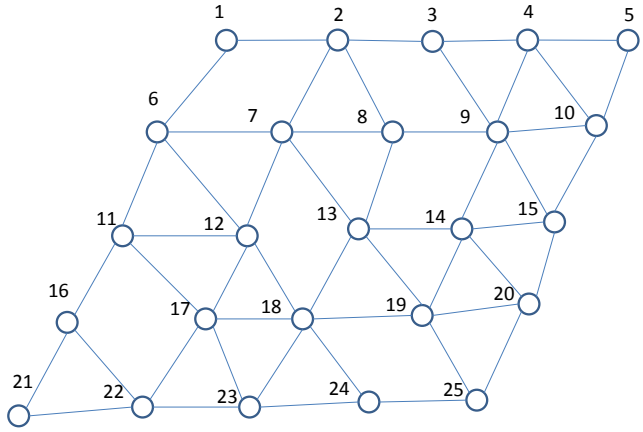

Fig. 11. Topology with 10% edges removed

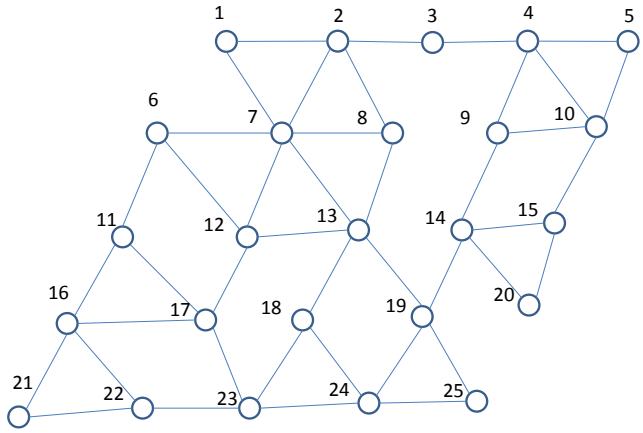

Fig. 12. Topology with 25% edges removed

AP can cover all the neighboring vertices in the graph and it can move to a neighboring vertex in every step. Fig 13 shows the original AP deployment of the network. Fig 14 and Fig 15 shows the AP distribution in two consecutive intervals. There are 9 APs A1, A2, ..., A9 distributed in the full triangular graph of 25 vertices. We can see that in interval 2, APs A1, A2, A4, A6, A7 and A9 move to a neighboring vertex and other APs remain in the same position. However, in both intervals all vertices in the graph are covered by at least one AP, assuming that every AP can cover its neighboring vertices.

SMT Solving Time of Topology Mutation with Different Topologies: Fig 16 shows the time for the SMT solver to find the satisfying AP movement scheduling of 10 intervals with different size of topology and number of edges. The number in the x-axis is the length of the mesh topology. For example, length 20 means a 20 by 20 mesh (with a total of 400 vertices in the graph). We can see that the solving time increases with the size of the topology. However we can see that the SMT solver can solve the mutation scheduling for a topology with up to 2500 vertices, and we believe that there is much room of improvement for SMT solvers. Also, the solving time is not affected very much for different number of removed edges.

SMT Solving Time of Topology Mutation with Different Number of APs: Fig 17 shows the time for the SMT solver to find the satisfying AP movement scheduling in a 30 by 30 topology with different number of APs. We can see that the solving time increase about linearly.

SMT Solving Time of Topology Mutation with Different Number of Intervals: Fig 18 shows the time for the SMT solver to find the satisfying AP movement with different number of intervals. We can see that the solving time increase exponentially with the number of scheduling intervals. However, in real applications the controller only needs to schedule a small number of intervals ahead of time and reschedule after a small number of intervals.

VII. Related Works

Cyber agility is an important research topic in recent years. It provides a proactive defense to deter many attacks including worm, botnet, DoS and renaissance attacks with the presence of uncertainties of the timing and types of attacks. The work in [5] presents the framework of random host IP mutation (RHM). In RHM, moving target hosts are assigned virtual IP addresses that change randomly and synchronously in a distributed fashion over time without disrupting active connections. IPv6 based mutation is investigated in [11] to leverage the immense address space of IPv6. The work in [10]

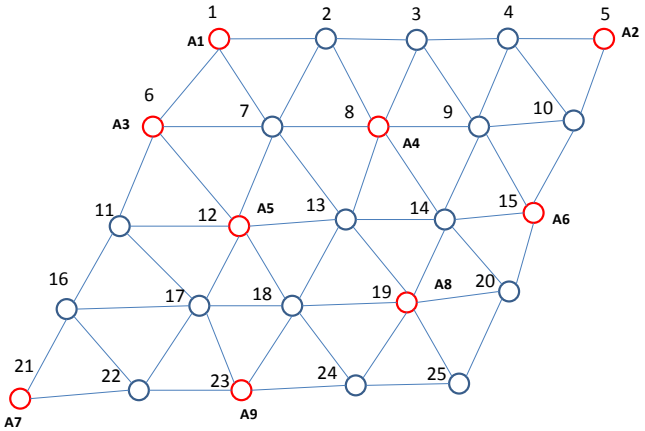

Fig. 13. AP layout in Interval 1

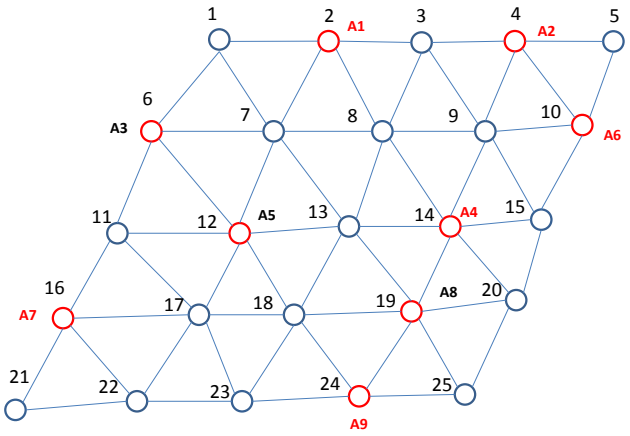

Fig. 14. AP layout in Interval 2

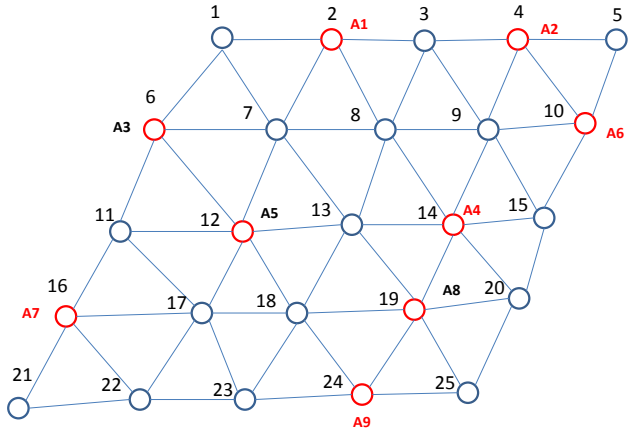

Fig. 15. AP layout in Interval 3

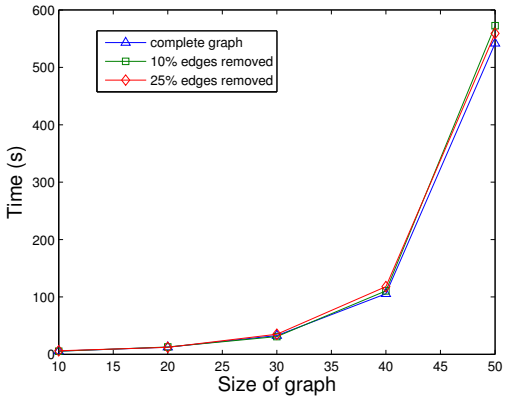

Fig. 16. Time to schedule AP motion with different topology sizes

presents Random Route Mutation (RRM) that enables changing randomly the route of the multiple flows in a network simultaneously to defend against reconnaissance, eavesdrop and DoS attacks, while preserving the required operational and security properties.

Agility in wireless/mobile networks is particularly interesting due to the intrinsic dynamic nature and special vulnerabilities of the wireless/mobile networks. The Software-defined radio (SDR) [2] is essentially an agile radio communication system which is flexible to avoid the limited spectrum of previous kinds of radios. The work in [13] applies a moving target defense to all nodes within a mobile-enabled system to provide security for critical nodes in the network.

Approaches for load balancing in a wireless local area network can be classified into two categories. One is association control through which the network re-distributes client associations among APs more or less uniformly so that no one AP is unduly overloaded [7], [15], [18]. The other is capacity control through which the network adjusts the maximum allowable throughput of each AP so that heavy-loaded APs can have more capacity to support users [17]. However, these works are not from the security perspective.

VIII. Conclusion and Future Work

In this paper, we investigate two wireless agility techniques: (1) Random Range Mutation (RNM) that allows for periodic changes of AP coverage range randomly, and (2) Random Topology Mutations (RTM) that allows for random motion and placement of APs in the wireless infrastructure. We apply SMT based formal framework to schedule the satisfying wireless AP mutation considering coverage, security, and energy constraints. Our evaluation shows that the AP mutation techniques can effectively defend against eavesdrop and DoS attacks, with reasonably performance degradation. The SMT based formalization can solve mutation scheduling in topologies as large as 2500 vertices, and the throughput reduction is less than 2%. Compared with the case of no mutation, the percentage of compromised flows can decrease by more than 90%.

The AP mutation should also maintain the connectivity among the APs if they form an ad hoc network. In the current formalization we do not include connectivity constraint since we assume there are a large number of APs and connectivity can be easily satisfied even if a percentage of APs are inactive in a given interval. If there is not enough number of APs or the percentage of inactive APs is large in a given interval, then we need to consider connectivity constraints. This is one direction

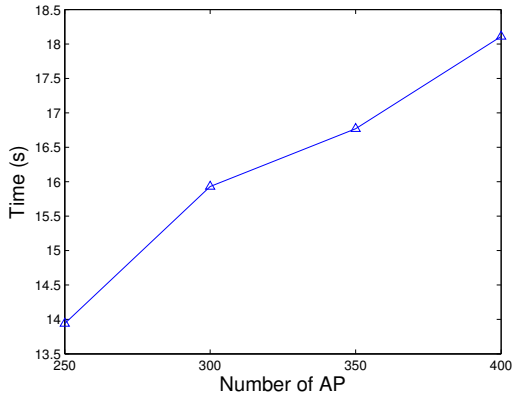

Fig. 17. Time to schedule AP motion of different number of APs

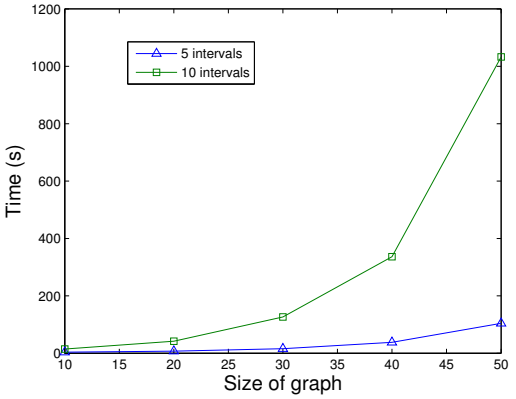

Fig. 18. Time to schedule AP motion in different intervals

of future work.

Another important limitation of the presented approaches is that the action of APs may directly impact the the adversary strategies. For example, when an AP changes its coverage range or location, an adaptive adversary may also react accordingly by changing its own locations or attacking targets. In the future, we plan to extend the research to game theory based wireless agility to consider the mutual interaction between defenders and attackers.

REFERENCES

[1] IAPP. https://www.privacyassociation.org/.

[2] A software-defined radio for the masses. https://sites.google.com/site/thesdrinstitute/A-Software-Defined-Radio-for-the-Masses.

[3] Yices: An SMT solver. http://yices.csl.sri.com/.

[4] IEEE 802.11k/D0.7. IEEE 802.11 WG draft supplement — specification for radio resource measurement.

[5] Ehab Al-Shaer, Qi Duan, and Jafar Haadi Jafarian. Random host mutation for moving target defense. In *Proceedings of the 8th International Conference on Security and Privacy in Communication Networks*, 2012.

[6] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. Reed. Femtocells: Past, present, and future. *IEEE J. Select. Areas Commun.*, 30(3):497–508, April 2012.

[7] Y. Bejerano, H. Seung-Jae, and L. Li. Fairness and load balancing in wireless lans using association control. *Networking, IEEE/ACM Transactions on*, 15(3):560–573, June 2007.

[8] N. Bjørner and L. de Moura. $z3^{10}$: Applications, enablers, challenges and directions. In *CFV '09 Sixth International Workshop on Constraints in Formal Verification*, 2009.

[9] U. Blumenthal and B. Wijnen. User-based security model (usm) for version 3 of the simple network management protocol (snmpv3), 1999.

[10] Qi Duan, Haadi Jafarian, and Ehab Al-Shaer. Efficient random route mutation considering flow and network constraints. In *IEEE CNS 2013*, 2013.

[11] Matthew Dunlop, Stephen Groat, William Urbanski, Randy Marchany, and Joseph Tront. Mt6d: A moving target ipv6 defense. In *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011*, pages 1321–1326, Nov 2011.

[12] A. Ghosh, J. G. Andrews, N. Mangalvedhe, R. Ratasuk, B. Mondal, M. Cudak, E. Visotsky, T. A. Thomas, P. Xia, H. S. Jo, H. S. Dhillon, and T. D. Novlan. Heterogeneous cellular networks: From theory to practice. *IEEE Commun. Mag.*, 50(6):54–64, June 2012.

[13] S. Groat, R. Moore, R. Marchany, and J. Tront. Securing static nodes in mobile-enabled systems using a network-layer moving target defense. In *Engineering of Mobile-Enabled Systems (MOBS), 2013 1st International Workshop on the*, pages 42–47, May 2013.

[14] D. Harrington, R. Presuhn, and B. Wijnen. An architecture for describing simple network management protocol (snmp) management frameworks, 2002.

[15] A. Hills and B. Friday. Radio resource management in wireless lans. *Communications Magazine, IEEE*, 42(12):9–14, Dec 2004.

[16] Sung-Ju Lee and Mario Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks (citations: 570). In *IEEE International Conference on Communications - ICC*, pages 3201–3205, 2001.

[17] Y. Matsunaga and R.H. Katz. Inter-domain radio resource management for wireless LANs. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, volume 4, pages 2183–2188 Vol.4, March 2004.

[18] K. Minkyong, L. Zhen, S. Parthasarathy, D. Pendarakis, and Y. Hao. Association control in mobile wireless networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages –, April 2008.

[19] Arunesh Mishra, Minho Shin, and William Arbaugh. An empirical analysis of the ieee 802.11 mac layer handoff process. *SIGCOMM Comput. Commun. Rev.*, 33(2):93–102, April 2003.

[20] T. Q. S. Quek, G. de la Roche, I. Guvenc, and M. Kountouris. *Small Cell Networks: Deployment, PHY Techniques, and Resource Management*. Cambridge University Press, 2013.

[21] Jiang Xie, I. Howitt, and I. Shibeika. Ieee 802.11-based mobile ip fast handoff latency analysis. In *Communications, 2007. ICC '07. IEEE International Conference on*, pages 6055–6060, June 2007.

[22] Zhenqiang Ye, Srikanth V. Krishnamurthy, and Satish K. Tripathi. A framework for reliable routing in mobile ad hoc networks. In *IEEE INFOCOM*, pages 270–280, 2003.